Caring is Sharing – Exploiting the Value in Data for Health and Innovation
M. Hägglund et al. (Eds.)

doi:10.3233/SHTI230130

MedSecurance Project: Advanced Security-for-Safety Assurance for Medical Device IoT (IoMT)

Parisis GALLOS[a,1], Rance DeLONG[b], Nicholas MATRAGKAS[c], Allan BLANCHARD[c], Chokri MRAIDHA[c] Gregory EPIPHANIOU[d], Carsten MAPLE[d], Konstantinos KATZIS[e], Jaime DELGADO[f], Silvia LLORENTE[f], Pedro MALÓ[g], Bruno ALMEIDA[g], Andreas MENYCHTAS[h], Christos PANAGOPOULOS[h], Ilias MAGLOGIANNIS[h], Petros PAPACHRISTOU[i], Mariana SOARES[j], Paula BREIA[j], Ana Cristina VIDAL[j], Martin RATZ[k], Ross WILLIAMSON[k], Eduard ERWEE[k], Lukasz STASIAK[k], Orfeu FLORES[l], Carla CLEMENTE[l], John MANTAS[a], Patrick WEBER[a], Theodoros N. ARVANITIS[m] and Scott HANSEN[b]

[a] *European Federation of Medical Informatics, Switzerland*
[b] *The Open Group, UK*
[c] *CEA, List, Université Paris-Saclay, France*
[d] *University of Warwick, UK*
[e] *European University Cyprus, Cyprus*
[f] *Universitat Politecnica de Catalunya, Spain*
[g] *Unparallel Innovation, Portugal*
[h] *BioAssist S.A., Greece*
[i] *HYGEIA Medical Group, Greece*
[j] *Centro Garcia de Orta, Hospital Garcia de Orta, Portugal*
[k] *Doccla AB, Sweden*
[l] *STAB VIDA, Portugal*
[m] *University of Birmingham, UK*

ORCiD ID: Parisis Gallos https://orcid.org/0000-0002-8630-7200, Rance DeLong https://orcid.org/0000-0002-6089-4734, Nicholas Matragkas https://orcid.org/0000-0002-8594-1912, Allan Blanchard https://orcid.org/0000-0001-7922-4880, Chokri Mraidha https://orcid.org/0000-0003-2993-5734, Dr Gregory Epiphaniou https://orcid.org/0000-0003-1054-6368, Konstantinos Katzis https://orcid.org/0000-0002-1470-2105, Jaime Delgado https://orcid.org/0000-0003-1366-663X, Silvia Llorente https://orcid.org/0000-0003-2000-6912, Pedro Maló https://orcid.org/0000-0001-6171-7345, Bruno Almeida https://orcid.org/0009-0001-0535-994X, Andreas Menychtas https://orcid.org/0000-0002-4510-5522, Christos Panagopoulos https://orcid.org/0000-0001-9282-0919, Ilias Maglogiannis https://orcid.org/0000-0003-2860-399X, Petros Papachristou https://orcid.org/0000-0001-5508-1934, Mariana Soares https://orcid.org/0000-0002-5538-334X, Paula Breia https://orcid.org/0000-0001-5188-9215, Ana Cristina Vidal https://orcid.org/0000-0002-3841-583X, Carla Clemente https://orcid.org/0000-0002-3384-4563, John

[1] Corresponding Author: Parisis Gallos, European Federation of Medical Informatics (EFMI), Ch de Maillefer 37, CH-1052 Le Mont-sur-Lausanne, Switzerland; E-mail: parisgallos@yahoo.com.

Mantas https://orcid.org/0000-0002-3051-1819, Patrick Weber https://orcid.org/0000-0003-4469-0464, Prof Theodoros N. Arvanitis https://orcid.org/0000-0001-5473-135X

Abstract. The MedSecurance project focus on identifying new challenges in cyber security with focus on hardware and software medical devices in the context of emerging healthcare architectures. In addition, the project will review best practice and identify gaps in the guidance, particularly the guidance stipulated by the medical device regulation and directives. Finally, the project will develop comprehensive methodology and tooling for the engineering of trustworthy networks of inter-operating medical devices, that shall have security-for-safety by design, with a strategy for device certification and certifiable dynamic network composition, ensuring that patient safety is safeguarded from malicious cyber actors and technology "accidents".

Keywords. Cyber Security, Medical Devices, IoT, Internet of Things

1. Introduction

According to the Annex I section 1 of the Medical Devices Regulation, both security and safety have to be considered for medical devices as patients' safety may be compromised due to "security issues" which may have "safety impacts" [1]. Weak security refers to security vulnerabilities that might be exploited to modify the normal behaviour of a medical device. On the other hand, restrictive security refers to very strict security measures that might affect the functional safety of a device [2]. Modern medical devices software development practices are the leading solutions to address complexity and evolution [3,4]. However, substantial challenges remain in achieving interoperability, dependability, and trustworthiness at scale within a diverse commercial medical device market facing an escalating threat environment. Meanwhile, advances in healthcare IT systems have resulted in complex socio-technical architectures, which deliver integrated and patient-centered services using medical devices. All these transformations, in addition to clinical benefits, they also introduce risks including security risks that need to be understood and managed to be reduced to acceptable levels [3]. There are numerous reports of new types of security vulnerabilities for this kind of architectures, which challenge the effectiveness of the current security tools [5-7].

MedSecurance envisages to address the identified challenges and go beyond the state-of-the-art by proposing a novel tool-supported methodology for safety-security co-analysis as part of a Threat Vulnerability Risk Analysis (TVRA) framework [8,9]. The proposed novel methodology will combine architectural and graph-based formalisms to model the system, possible attacks and failures, and how these propagate through the system components. The methodology will support the specification of the interdependencies between safety and security, and it will include interactions such as conflict between safety and security requirements, and conditional dependencies between the two. New metrics for quantifying the interaction of safety and security within a medical device will be proposed and they will support trade-off analysis.

2. MedSecurance Objectives and Approach

MedSecurance project will conceive novel methodologies, infrastructures, and technologies that enable an effective, harmonious and continuous development and evolution of secure system engineering management activities in Internet of Medical Things (IoMT). Project's main objective is to advance knowledge and basic understanding of decision making in diverse IoMT threat landscapes based on different system and component level interactions. This can be accomplished via the development of a novel holistic strategy that considers the interdependence of several IoMT subsystems, information exchange, risk thresholds, and regulatory ramifications. At this end, scalable and verifiable secure system engineering management solutions that capture, communicate, and act on these complexities in order to improve decision-making in cyber defense while automating cybersecurity assurance will be provided. Figure 1 illustrates the concept of MedSecurance.

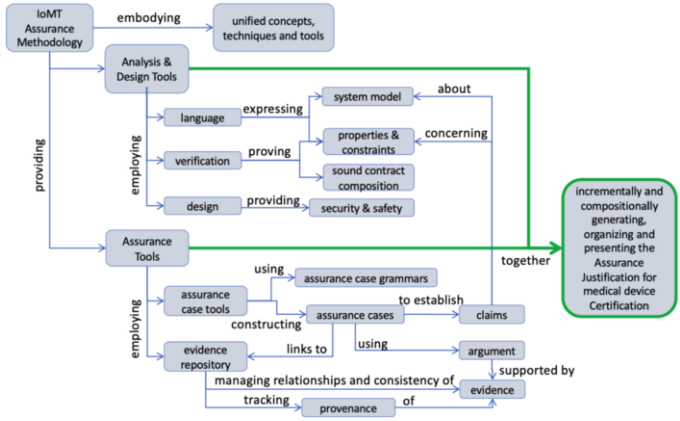

Figure 1. Concept of MedSecurance.

A stepwise approach will be used to achieve the project's main objective.

2.1. Systematic review, concept, and gap analysis of security approaches for the Internet of Medical Things (IoMT)

The project will perform a systematic review of security and safety standards and guidelines applicable to a) healthcare and b) health IT systems in general. The analysis will identify the main recommendations and concepts behind each standard and will perform a gap analysis with respect to the MDCG 2019-16 [10]. Furthermore, the standards and guidelines will be reviewed to identify gaps in the guidance with respect to the architectures and technologies identified in the first step. To proceed with Gaps mapping, a methodology that employs an iterative approach to reviewing and mapping the relevant documents and standards for inclusion in the full gap analysis process will be followed. Additionally, an elaboration and analysis of typical and alternative architectures for IoMT will be performed, to include system-driven risk-based threat modelling, vulnerability analysis, fault tree, Failure Mode and Effect Analysis (FMEA), and architectural patterns that substantially support specific classes of safety and security properties [11-13]. The purpose is to define and implement the appropriate TVRA processes and workflows based on best practices and compliant with existing legal and regulatory ramifications in both security engineering and resilience lines of effort.

2.2. Requirements and design of harmonized tools and methods for the unification of automated security and safety assurance for certification of IoMT

The project will examine modelling the integrated risk assessment approach proposed by ENISA [14], along with modelling the minimum viable security concepts required for assurance, which will be found in the literature. This will harmonize different security approaches and allow the transformation of terminology used in legacy certifications and the application of different standards. Assurance Automation design encompasses architectural, behavioural and communication modelling, semantic modelling (ontologies), modelling of essential characteristics, trust modelling of interfaces (contracts), as well as characterization of vulnerabilities analysis of design and implementation representations (design and code) to verify essential characteristics and marshalling of demonstrably sufficient evidence to support medical device safety/security certification (assurance cases).

2.3. Development of a security assurance automation toolbox

Develop assurance cases patterns and blueprints that are composable to demonstrate satisfaction of conformance with standards, regulations, legal obligations, and security-for-safety objectives by incorporating evidence from the architecture, design and implementation analyses of medical device connectivity solutions. In addition, the project will look at the interoperability software standards used in healthcare, and will implement interfaces that will assure the secure integration of components when their individual contracts are satisfied by their respective manufacturers. This will include developing of FHIR profiles for security assurance, and code security review and implementation of RESTful code (which is the main standard in healthcare). A related tool will allow the generation of secure code based on the different data exchange configurations.

2.4. Verification and Validation of the methods and tools by the Industry

Industry validation of new risk assessment and security assurance methods and tools will take place in the context of the MedSecurace. Pilot case evaluations by multiple Medical Devices suppliers under three project Use Cases for evaluating automated security assurance tools and methods. An appropriate architecture for implementing the process and enabling traceability between the system-level and component-level security requirements in IoMT via the programme will be developed.

2.5. MDCG 2019-16 recommendations, dissemination and engagement of stakeholders

The project will propose updates to the guidance that will bridge the gaps that will be identified. Furthermore, the project will expand the guidance, offering specific methods to be used (or references to standards) appropriate for each stage of the lifecycle and each architecture. Trade-off studies among alternative implementation technologies to inform choices will be needed to provide rationale for those choices. The proposed lifecycle and methods will correspond to a minimum assurance justification that will be identified by the prevailing certification authority. The project will incorporate a co-production approach identifying appropriate stakeholders who will offer knowledge and expertise,

including regulators, manufacturers as well as operators of medical devices and healthcare facilities.

3. Expected Outcomes - Conclusions

The MedSecurance provides a framework for ensuring proper security governance and empowering management to make security-aware choices about the evolving threats and risks in IoMT. A multi-layer Threat, Vulnerability and Risk Assessment (TVRA) approach will meant to be adaptable to any IoMT environment where the resilience lines of effort and security processes are entrenched but are specifically geared to risk identification, assessment, and treatment in order to allow the creation and management of security needs for such unique medical cyberinfrastructures. The proposed solutions will be co-developed and validated with our medical industry user partners, and complemented by engagement of healthcare industry stakeholders in support of the recommendations to existing guidelines that will also be developed in the project.

Acknowledgements

This work is co-funded by the HORIZON.2.1 - Health Programme of the European Commission, Grant Agreement number: 101095448 - Advanced Security-for-safety Assurance for Medical Device IoT (MEDSECURANCE).

References

[1] EU Regulation for Medical Devices. Available at: https://www.medical-device-regulation.eu/download-mdr/
[2] Katzis K, Jones RW, Despotou G. The Challenges of Balancing Safety and Security in Implantable Medical Devices. Stud Health Technol Inform. 2016;226:25-8.
[3] Despotou G, et al. A framework for synthesis of safety justification for digitally enabled healthcare services. Digit Health. 2017 Apr 24;3:2055207617704271.
[4] Czarnecki K. Requirements engineering in the age of societal-scale cyber-physical systems: The case of automated driving. In2018 IEEE 26th Intern Requirements Engineering Conf (RE) 2018 (pp. 3-4). IEEE.
[5] Yaacoub JP, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems. 2020 Sep 1;77:103201.
[6] Meng N, et al. Secure coding practices in java: Challenges and vulnerabilities. InProceedings of the 40th International Conference on Software Engineering 2018 May 27 (pp. 372-383).
[7] Ferrara P, Mandal AK, Cortesi A, Spoto F. Static analysis for discovering IoT vulnerabilities. International Journal on Software Tools for Technology Transfer. 2021 Feb;23:71-88.
[8] Threat, Vulnerability And Risk Assessment (TVRA). Available at: https://aipriskconsulting.com/theat-vulnerability-and-risk-assessment-tvra/
[9] Atay S, Masera M. Challenges for the security analysis of Next Generation Networks. Information security technical report. 2011 Feb 1;16(1):3-11.
[10] MDCG 2019-16 - Guidance on Cybersecurity for medical devices Available at: https://ec.europa.eu/docsroom/documents/41863.
[11] Ericson CA. Fault tree analysis. InSystem Safety Conference, Orlando, Florida 1999 (Vol. 1, pp. 1-9).
[12] Abdo H, et al. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. Computers & security. 2018 Jan 1;72:17595.
[13] Llorente S, Delgado J. Implementation of Privacy and Security for a Genomic Information System Based on Standards. J Pers Med. 2022 May 31;12(6):915. doi: 10.3390/jpm12060915.
[14] ENISA RM/RA Framework. Available at: https://www.enisa.europa.eu/topics/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework?v2=1&tab=details